

SOME SPECIAL FEATURES OF CAYLEY ALGEBRAS, AND G_2 , IN LOW CHARACTERISTICS

ALONSO CASTILLO-RAMIREZ* AND ALBERTO ELDUQUE**

ABSTRACT. Some features of Cayley algebras (or algebras of octonions) and their Lie algebras of derivations over fields of low characteristic are presented. More specifically, over fields of characteristic 7, explicit embeddings of any twisted form of the Witt algebra into the simple split Lie algebra of type G_2 are given. Over fields of characteristic 3, even though the Lie algebra of derivations of a Cayley algebra is not simple, it is shown that still two Cayley algebras are isomorphic if and only if their Lie algebras of derivations are isomorphic. Finally, over fields of characteristic 2, it is shown that the Lie algebra of derivations of any Cayley algebra is always isomorphic to the projective special linear Lie algebra of degree four. The twisted forms of this latter algebra are described too.

1. INTRODUCTION

Let \mathbb{F} be an arbitrary field. Cayley algebras (or algebras of octonions) over \mathbb{F} constitute a well-known class of nonassociative algebras (see, e.g. [KMRT98, Chapter VIII] and references therein). They are unital nonassociative algebras \mathcal{C} of dimension eight over \mathbb{F} , endowed with a nonsingular quadratic multiplicative form (the *norm*) $q : \mathcal{C} \rightarrow \mathbb{F}$. Hence $q(xy) = q(x)q(y)$ for any $x, y \in \mathcal{C}$, and the polar form $b_q(x, y) := q(x + y) - q(x) - q(y)$ is a nondegenerate bilinear form.

Any element in a Cayley algebra \mathcal{C} satisfies the degree 2 equation:

$$x^2 - b_q(x, 1)x + q(x)1 = 0. \quad (1)$$

Besides, the map $x \mapsto \bar{x} := b_q(x, 1)1 - x$ is an involution (i.e., an antiautomorphism of order 2) and the *trace* $t(x) := b_q(x, 1)$ and norm $q(x)$ are given by $t(x)1 = x + \bar{x}$, $q(x)1 = x\bar{x} = \bar{x}x$ for any $x \in \mathcal{C}$. Two Cayley algebras \mathcal{C}_1 and \mathcal{C}_2 , with respective norms q_1 and q_2 , are isomorphic if and only if the norms q_1 and q_2 are isometric.

If the characteristic of \mathbb{F} is not 2, then $\mathcal{C} = \mathbb{F}1 \oplus \mathcal{C}^0$, where \mathcal{C}^0 is the subspace of trace zero elements (i.e., the subspace orthogonal to $\mathbb{F}1$ relative to b_q). For $x, y \in \mathcal{C}^0$, (1) shows that $xy + yx = -b_q(x, y)1$, while $t([x, y]) = [x, y] + [\bar{x}, \bar{y}] = [x, y] + [\bar{y}, \bar{x}] = 0$, so $[x, y] := xy - yx \in \mathcal{C}^0$. In particular,

$$xy = -\frac{1}{2}b_q(x, y)1 + \frac{1}{2}[x, y], \quad (2)$$

so the projection of xy in \mathcal{C}^0 is $\frac{1}{2}[x, y]$. Moreover, the following relation holds (see, e.g. [EK13, Theorem 4.23]):

$$[[x, y], y] = 2b_q(x, y)y - 2b_q(y, y)x, \quad (3)$$

so the multiplication in \mathcal{C} and its norm are determined by the bracket in \mathcal{C}^0 .

2010 *Mathematics Subject Classification.* Primary 17A75; Secondary 17B60, 17B25.

Key words and phrases. Octonions; Cayley algebra; Derivations; G_2 .

* Supported by the 150th Anniversary Postdoctoral Mobility Grant (PMG14-15 01) of the London Mathematical Society.

** Supported by the Spanish Ministerio de Economía y Competitividad—Fondo Europeo de Desarrollo Regional (FEDER) MTM2013-45588-C3-2-P, and by the Diputación General de Aragón—Fondo Social Europeo (Grupo de Investigación de Álgebra).

The Lie algebra of derivations of a Cayley algebra \mathcal{C} is defined by

$$\text{Der}(\mathcal{C}) := \{d \in \mathfrak{gl}(\mathcal{C}) : d(xy) = d(x)y + xd(y) \ \forall x, y \in \mathcal{C}\}.$$

In general, if M is a module for a Lie algebra \mathcal{L} , we say that a bilinear product $\cdot : M \times M \rightarrow M$ is \mathcal{L} -invariant if \mathcal{L} acts on (M, \cdot) by derivations: $x(u \cdot v) = x(u) \cdot v + u \cdot x(v)$, for any $x \in \mathcal{L}$, $u, v \in M$.

If the norm q of a Cayley algebra \mathcal{C} is isotropic (i.e., there exists $0 \neq x \in \mathcal{C}$ with $q(x) = 0$), then \mathcal{C} is unique up to isomorphism. In this case, the Cayley algebra \mathcal{C} is said to be *split*, and it has a *good basis* $\{p_1, p_2, u_1, u_2, u_3, v_1, v_2, v_3\}$ with multiplication given in Table 1. We denote by \mathcal{C}_s the split Cayley algebra.

	p_1	p_2	u_1	u_2	u_3	v_1	v_2	v_3
p_1	p_1	0	u_1	u_2	u_3	0	0	0
p_2	0	p_2	0	0	0	v_1	v_2	v_3
u_1	0	u_1	0	v_3	$-v_2$	$-p_1$	0	0
u_2	0	u_2	$-v_3$	0	v_1	0	$-p_1$	0
u_3	0	u_3	v_2	$-v_1$	0	0	0	$-p_1$
v_1	v_1	0	$-p_2$	0	0	0	u_3	$-u_2$
v_2	v_2	0	0	$-p_2$	0	$-u_3$	0	u_1
v_3	v_3	0	0	0	$-p_2$	u_2	$-u_1$	0

TABLE 1. Multiplication table in a good basis of the split Cayley algebra.

Given a finite-dimensional simple Lie algebra \mathfrak{g} of type X_r over the complex numbers, and a Chevalley basis \mathcal{B} , let $\mathfrak{g}_{\mathbb{Z}}$ be the \mathbb{Z} -span of \mathcal{B} (a Lie algebra over \mathbb{Z}). The Lie algebra $\mathfrak{g}_{\mathbb{F}} := \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}$ is the *Chevalley algebra* of type X_r . In particular, the Chevalley algebra of type G_2 is isomorphic to $\text{Der}(\mathcal{C}_s)$ (see, e.g. [EK13, §4.4]). For any Cayley algebra \mathcal{C} , the Lie algebra $\text{Der}(\mathcal{C})$ is a twisted form of the Chevalley algebra $\text{Der}(\mathcal{C}_s)$. (Recall that, if \mathcal{A} and \mathcal{B} are algebras over \mathbb{F} , then \mathcal{A} is a *twisted form* of \mathcal{B} whenever $\mathcal{A} \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}} \cong \mathcal{B} \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}$, for an algebraic closure \mathbb{F}_{alg} of \mathbb{F} .)

If the characteristic of \mathbb{F} is neither 2 nor 3, then the Chevalley algebra of type G_2 is simple; this is the split simple Lie algebra of type G_2 . Moreover, two Cayley algebras \mathcal{C}_1 and \mathcal{C}_2 are isomorphic if and only if their Lie algebras of derivations are isomorphic (see [Sel67, Theorem IV.4.1] or [EK13, Theorem 4.35]).

The goal of this paper is to show some surprising features of Cayley algebras over fields of characteristic 7, 3 and 2.

Section 2 studies the case of characteristic 7 and is divided in three subsections. In Section 2.1, we review a construction of \mathcal{C}_s due to Dixmier [Dix84] in terms of transvectants which was originally done in characteristic 0, but it is valid in any characteristic $p \geq 7$. In this construction, \mathcal{C}_s appears as the direct sum of the trivial one-dimensional module and the restricted irreducible seven-dimensional module V_6 for the simple Lie algebra $\mathfrak{sl}_2(\mathbb{F})$, which embeds into $\text{Der}(\mathcal{C}_s)$ as its principal \mathfrak{sl}_2 subalgebra. When the characteristic is 7, this action of $\mathfrak{sl}_2(\mathbb{F})$ by derivations on \mathcal{C}_s may be naturally extended to an action by derivations of the Witt algebra $W_1 := \text{Der}(\mathbb{F}[X]/(X^7))$, explaining the fact, first proved in [Pre83, Lemma 13] (see also [HSpr]), that W_1 embeds into the split simple Lie algebra of type G_2 . In Section 2.2, we show that, when \mathbb{F} is algebraically closed, V_6 is the unique non-trivial non-adjoint restricted irreducible module for W_1 with a nonzero invariant product.

Then, in Section 2.3 we prove that, in characteristic 7 and even when the ground field is not algebraically closed, all the twisted forms of the Witt algebra embed into $\text{Der}(\mathcal{C}_s)$, and any two embeddings of the same twisted form are conjugate by an automorphism.

Section 3 is devoted to the case of characteristic 3. In this situation, it is known that the Chevalley algebra of type G_2 is not simple, but it contains an ideal isomorphic to the projective special linear Lie algebra $\mathfrak{psl}_3(\mathbb{F})$. We review this situation and prove that it is still valid that two Cayley algebras are isomorphic if and only if their Lie algebras of derivations are isomorphic.

Finally, in Section 4, we prove that the Lie algebra of derivations $\text{Der}(\mathcal{C})$ of any Cayley algebra \mathcal{C} over a field \mathbb{F} of characteristic 2 is always isomorphic to the projective special linear Lie algebra $\mathfrak{psl}_4(\mathbb{F})$. A proof of this fact when $\mathcal{C} = \mathcal{C}_s$ appears in [EK13, Corollary 4.32]. Hence, in this case, it is plainly false that two Cayley algebras are isomorphic if and only if their Lie algebras of derivations are isomorphic. We show that the isomorphism classes of twisted forms of $\mathfrak{psl}_4(\mathbb{F})$, which is here the Chevalley algebra of type G_2 , are in bijection with the isomorphism classes of central simple associative algebras of degree 6 endowed with a symplectic involution.

2. CHARACTERISTIC 7

2.1. Dixmier's construction. Let $\mathbb{F}[x, y]$ be the polynomial algebra in two variables over a field \mathbb{F} of characteristic 0. The general linear Lie algebra $\mathfrak{gl}_2(\mathbb{F})$ acts by derivations on $\mathbb{F}[x, y]$ preserving the degree of each polynomial. For any $n \geq 0$, denote by V_n the subspace of homogeneous polynomials of degree n in $\mathbb{F}[x, y]$. For any $i, j, q \geq 0$ with $q \leq i, j$, consider the q -transvectant $V_i \times V_j \rightarrow V_{i+j-2q}$ given by

$$(f, g)_q := \frac{(i-q)!}{i!} \frac{(j-q)!}{j!} \left(\frac{\partial^q f}{\partial x^q} \frac{\partial^q g}{\partial y^q} - \binom{q}{1} \frac{\partial^q f}{\partial x^{q-1} \partial y} \frac{\partial^q g}{\partial x \partial y^{q-1}} + \binom{q}{2} \frac{\partial^q f}{\partial x^{q-2} \partial y^2} \frac{\partial^q g}{\partial x^2 \partial y^{q-2}} - \dots \right),$$

for $f \in V_i$ and $g \in V_j$.

It turns out that the split Cayley algebra \mathcal{C}_s is isomorphic to the algebra defined on $\mathbb{F}1 \oplus V_6$ with multiplication given by

$$(\alpha 1 + f)(\beta 1 + g) := (\alpha\beta - \frac{1}{20}(f, g)_6)1 + (\alpha g + \beta f + (f, g)_3), \quad (4)$$

for any $\alpha, \beta \in \mathbb{F}$ and $f, g \in V_6$ (see [Dix84, 3.6 Proposition]); equipped with this product, the subspace V_6 becomes the subspace of trace zero elements in \mathcal{C}_s . The existence of this isomorphism is based on the following identity given in [Dix84, 3.5 Lemme]:

$$((f, g)_3, g)_3 = \frac{1}{20}((f, g)_6 g - (g, g)_6 f), \quad (5)$$

for any $f, g \in V_6$.

Consider the following endomorphisms of V_6 :

$$e_{-1} := x \frac{\partial}{\partial y} \Big|_{V_6}, \quad e_0 := -\frac{1}{2} \left(x \frac{\partial}{\partial x} - y \frac{\partial}{\partial y} \right) \Big|_{V_6}, \quad e_1 := -y \frac{\partial}{\partial x} \Big|_{V_6}.$$

A direct calculation gives $[e_i, e_j] = (j-i)e_{i+j}$, for $i, j \in \{-1, 0, 1\}$, so these endomorphisms span a subalgebra of $\mathfrak{gl}(V_6)$ isomorphic to $\mathfrak{sl}_2(\mathbb{F})$ that acts by derivations on V_6 . This construction also works when the characteristic of \mathbb{F} is $p \geq 7$, and, moreover, the map $f \otimes g \mapsto (f, g)_3$ gives the only, up to scalars, linear map $V_6 \otimes V_6 \rightarrow V_6$ invariant under the action of $\mathfrak{sl}_2(\mathbb{F})$.

Now assume that the characteristic of \mathbb{F} is 7. First, we will find a simpler formula describing the 3-transvectant $(\cdot, \cdot)_3 : V_6 \times V_6 \rightarrow V_6$. For $0 \leq i \leq 6$, denote

$$m_i := x^{6-i}y^i \in V_6.$$

Taking the indices modulo 7, the action of $\mathfrak{sl}_2(\mathbb{F})$ on V_6 is given by the following formulas:

$$\begin{aligned} e_{-1}(m_i) &= im_{i-1} \text{ for } 1 \leq i \leq 6, \text{ and } e_{-1}(m_0) = 0, \\ e_0(m_i) &= (i+4)m_i \text{ for any } 0 \leq i \leq 6, \\ e_1(m_i) &= (i+1)m_{i+1} \text{ for } 0 \leq i \leq 5, \text{ and } e_1(m_6) = 0. \end{aligned} \quad (6)$$

For i, j in the prime subfield \mathbb{F}_7 of \mathbb{F} , define the element $c(i, j)$ by

$$c(i, j) = 2(j-i)(4i+j-1)(4j+i-1) \pmod{7}. \quad (7)$$

It is clear that $c(i, j) = -c(j, i)$ for any $i, j \in \mathbb{F}_7$, and $c(0, 6) = 1$. A straightforward computation gives, for any $i, j, k \in \mathbb{F}_7$:

$$(i+j+4k+1)c(i, j) = (i+4k+4)c(i+k, j) + (j+4k+4)c(i, j+k). \quad (8)$$

Therefore, defining

$$m_i \cdot m_j := c(i, j)m_{i+j-3} \quad (9)$$

(with indices modulo 7), we have

$$e_k(m_i \cdot m_j) = e_k(m_i) \cdot m_j + m_i \cdot e_k(m_j),$$

for any $k \in \{-1, 0, 1\}$, $0 \leq i, j \leq 6$. This means that the product in (9) is $\mathfrak{sl}_2(\mathbb{F})$ -invariant; hence, by uniqueness and since $(m_0, m_6)_3 = m_3 = m_0 \cdot m_6$, we conclude that

$$m_i \cdot m_j = (m_i, m_j)_3 \quad (10)$$

for any $0 \leq i, j \leq 6$. The multiplication table of V_6 with this product is given in Table 2.

\cdot	m_0	m_1	m_2	m_3	m_4	m_5	m_6
m_0	0	0	0	$-m_0$	$3m_1$	$-3m_2$	m_3
m_1	0	0	$3m_0$	m_1	0	$-m_3$	$-3m_4$
m_2	0	$-3m_0$	0	m_2	$-m_3$	0	$3m_5$
m_3	m_0	$-m_1$	$-m_2$	0	m_4	m_5	$-m_6$
m_4	$-3m_1$	0	m_3	$-m_4$	0	$3m_6$	0
m_5	$3m_2$	m_3	0	$-m_5$	$-3m_6$	0	0
m_6	$-m_3$	$3m_4$	$-3m_5$	m_6	0	0	0

TABLE 2. Multiplication table of (V_6, \cdot) .

Remark 1. The above arguments show that the split Cayley algebra \mathcal{C}_s is isomorphic to the algebra defined on $\mathbb{F}1 \oplus V_6$ with multiplication given by (4), or equivalently, by

$$(\alpha 1 + f)(\beta 1 + g) := (\alpha\beta + (f, g)_6)1 + (\alpha g + \beta f + f \cdot g).$$

An explicit isomorphism between $\mathbb{F}1 \oplus V_6$ and \mathcal{C}_s , in terms of a good basis of \mathcal{C}_s as in Table 1, is given by:

$$\begin{pmatrix} 1 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ p_1 + p_2 & -3v_3 & 3u_2 & 3u_1 & -p_1 + p_2 & -3v_1 & -3v_2 & 3u_3 \end{pmatrix}.$$

Now, for any $k \in \{2, \dots, 5\}$, define the endomorphism e_k of V_6 by

$$e_k(m_i) = \begin{cases} (i + 4k + 4)m_{i+k} & \text{if } i + k \leq 6, \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

We will show that e_k is a derivation of (V_6, \cdot) for any $k = \{-1, 0, \dots, 5\}$. Take $0 \leq i, j \leq 6$. If $i + j + k - 3 \leq 6$, $i + k \leq 6$, and $j + k \leq 6$, then

$$\begin{aligned} e_k(m_i \cdot m_j) &= (i + j + 4k + 1)c(i, j)m_{i+j+k-3} \\ &= \left((i + 4k + 4)c(i + k, j) + (j + 4k + 4)c(i, j + k) \right) m_{i+j+k-3} \\ &= e_k(m_i) \cdot m_j + m_i \cdot e_k(m_j). \end{aligned} \quad (12)$$

If $i + j + k - 3 > 6$, then $e_k(m_i \cdot m_j) = 0 = e_k(m_i) \cdot m_j = m_i \cdot e_k(m_j)$. Finally, if $i + j + k - 3 \leq 6$ and $i + k > 6$ (the same happens if $j + k > 6$), then $e_k(m_i) = 0$ and $c(i + k, j)$ is one of $c(0, 0)$, $c(0, 1)$, $c(0, 2)$ or $c(1, 1)$, but all these are equal to 0, so (12) applies.

Because of (4) and (5), we may extend the action of e_k to $\mathbb{F}1 \oplus V_6 \cong \mathcal{C}_s$ by means of $e_k(1) = 0$, obtaining that e_k is a derivation of the split Cayley algebra \mathcal{C}_s . Furthermore, one checks at once that

$$[e_i, e_j] = (j - i)e_{i+j} \quad (13)$$

for any $i, j \in \{-1, 0, \dots, 5\}$, with $e_i = 0$ when i is outside $\{-1, 0, \dots, 5\}$. Thus, the span of $\{e_i : -1 \leq i \leq 5\}$ in $\text{Der}(V_6, \cdot)$ is isomorphic to the Witt algebra $W_1 := \text{Der}(\mathbb{F}[X]/(X^7))$; the map $e_i \leftrightarrow x^{i+1} \frac{\partial}{\partial x}$ gives an explicit isomorphism of these Lie algebras, where x denotes the class of X modulo (X^7) .

Since $\text{Der}(\mathcal{C}_s)$ is the split simple Lie algebra of type G_2 , the above arguments provide an elementary proof of the next result.

Theorem 2 ([Pre83]). *If the characteristic of the ground field \mathbb{F} is 7, then the Witt algebra W_1 embeds as a subalgebra of the simple split Lie algebra of type G_2 .*

Remark 3. A specific embedding of W_1 into $\text{Der}(\mathcal{C}_s)$ may be given in terms of a good basis of \mathcal{C}_s . Given $x, y \in \mathcal{C}_s$, the derivation of \mathcal{C}_s defined by $D_{x,y} := \text{ad}_{[x,y]} + [\text{ad}_x, \text{ad}_y]$ (where $\text{ad}_x(y) := [x, y]$) is called the *inner derivation induced by x and y* . Then, the assignment

$$\begin{aligned} e_{-1} &\mapsto D_{p_1-p_2, u_1} + D_{u_2, v_1}, & e_3 &\mapsto -D_{v_1, v_2} = 4D_{p_1-p_2, u_3}, \\ e_0 &\mapsto 2D_{u_3, v_3} + 3D_{u_2, v_2}, & e_4 &\mapsto 3D_{v_1, u_3}, \\ e_1 &\mapsto D_{p_1-p_2, v_1} + D_{u_1, v_2}, & e_5 &\mapsto 5D_{v_2, u_3}, \\ e_2 &\mapsto 3D_{u_1, u_3} = 2D_{p_1-p_2, v_2}, \end{aligned}$$

gives an explicit embedding of W_1 into $\text{Der}(\mathcal{C}_s)$.

2.2. Invariant bilinear products on modules for W_1 . It turns out that V_6 is a very special module for the Witt algebra in characteristic 7 (see Theorem 4 below).

Assume for this section that \mathbb{F} is an algebraically closed field of characteristic $p \geq 5$. Let \mathcal{L} be a finite-dimensional restricted Lie algebra over \mathbb{F} with p -mapping denoted by $[p]$. Given any character $\chi \in \mathcal{L}^*$, there is a finite-dimensional algebra $u(\mathcal{L}, \chi)$, called the *reduced enveloping algebra of \mathcal{L} associated with χ* , that is a quotient of the universal enveloping algebra of \mathcal{L} and whose irreducible modules coincide precisely with the irreducible modules for \mathcal{L} with character χ . We say that V is a *restricted module* for \mathcal{L} if there is a representation $\rho : \mathcal{L} \rightarrow \mathfrak{gl}(V)$ that is a morphism of restricted Lie algebras, i.e., $\rho(x^{[p]}) = \rho(x)^p$, for any $x \in \mathcal{L}$. When $\chi = 0$, it turns out that the irreducible modules for $u(\mathcal{L}, \chi)$ coincide precisely with the restricted irreducible modules for \mathcal{L} .

Let $W = W_1$ be the Witt algebra over \mathbb{F} with basis $\{e_i : -1 \leq i \leq p-2\}$ and Lie bracket as in (13). It is well known that W has a p -mapping given by $e_i^{[p]} := \delta_{i,0} e_i$.

For each $i \in \{-1, 0, \dots, p-2\}$, define $W_{(i)} = \langle e_i, \dots, e_{p-2} \rangle$. Consider the p -dimensional Verma modules $L(\lambda) = u(W, 0) \otimes_{u(W_{(0)}, 0)} k_\lambda$, where $\lambda \in \{0, 1, \dots, p-1\}$, and k_λ is the one-dimensional module for $W_{(0)}$ on which $W_{(1)}$ acts trivially and e_0 acts by multiplication by λ . By [Nak92, Lemma 2.2.1], $L(\lambda)$ has a basis $\{m_0, m_1, \dots, m_{p-1}\}$ on which the action of W is given by

$$e_k(m_j) = (j + (\lambda + 1)(k + 1))m_{k+j},$$

where $m_j = 0$ for j outside $\{0, \dots, p-1\}$.

It was established in [Cha41] (see also [Str77, FN98]) that any restricted irreducible module for W is isomorphic to one of the following:

- (1) The trivial one-dimensional module.
- (2) The $(p-1)$ -dimensional quotient $L(p-1)/\langle m_0 \rangle$.
- (3) The p -dimensional Verma module $L(\lambda)$, with $\lambda \in \{1, \dots, p-2\}$.

In the next result the invariant bilinear products $L \times L \rightarrow L$ (not to be confused with invariant bilinear forms!) on irreducible restricted modules for the Witt algebra are determined.

Theorem 4. *Let $W = W_1$ be the Witt algebra over an algebraically closed field \mathbb{F} of characteristic $p \geq 5$. Then:*

- (1) *If $p \neq 7$, there is no non-trivial non-adjoint restricted irreducible module for W with a nonzero invariant bilinear product.*
- (2) *If $p = 7$, there is a unique non-trivial non-adjoint restricted irreducible module for W with a nonzero invariant bilinear product. Up to isomorphism and scaling of the product, this unique module is V_6 with product given in (9). (V_6 is a module for W by means of (6) and (11).)*

Proof. We will use the above classification of restricted irreducible modules for W and follow several steps:

- (i) Let $\lambda \in \{0, 1, \dots, p-1\}$ and suppose that $L(\lambda)$ is equipped with \cdot , a W -invariant bilinear product. We claim that $m_0 \cdot m_{p-1} = \mu m_\lambda$, for some scalar $\mu \in \mathbb{F}$ that determines the invariant product. Indeed, first observe that

$$\begin{aligned} e_0(m_0 \cdot m_{p-1}) &= (\lambda + 1)m_0 \cdot m_{p-1} + (p-1 + (\lambda + 1))m_0 \cdot m_{p-1} \\ &= (2\lambda + 1)m_0 \cdot m_{p-1}. \end{aligned}$$

Therefore, $m_0 \cdot m_{p-1}$ is an eigenvector of the action of e_0 with eigenvalue $2\lambda + 1$. As m_λ is also an eigenvector of the action of e_0 with eigenvalue $2\lambda + 1$, and the action of e_0 is diagonal with p distinct eigenvalues, we must have that $m_0 \cdot m_{p-1}$ is a scalar multiple of m_λ . Furthermore, $m_0 \otimes m_{p-1}$ generates the W -module $L(\lambda) \otimes L(\lambda)$, so this scalar determines the invariant product.

- (ii) For any $p \geq 5$, we will show that if \cdot is a W -invariant bilinear product on the irreducible module $L(p-1)/\langle m_0 \rangle$, then it must be the zero product. Denote by \bar{x} the class of an element $x \in L(p-1)$ modulo $\langle m_0 \rangle$; then,

$$e_0(\bar{m}_1 \cdot \bar{m}_{p-1}) = \bar{m}_1 \cdot \bar{m}_{p-1} + (p-1)\bar{m}_1 \cdot \bar{m}_{p-1} = \bar{0}.$$

As all the eigenvalues of the action of e_0 on $L(p-1)/\langle m_0 \rangle$ are nonzero, this implies that $\bar{m}_1 \cdot \bar{m}_{p-1} = \bar{0}$. Now, using the W -invariance, it is easy to show that \cdot must be the zero product.

- (iii) As $L(p-2)$ is the adjoint module for W , it obviously has a W -invariant bilinear product. Hence, we exclude this case from further observations.

- (iv) Let $p \geq 5$ and $\lambda \in \{1, \dots, p-3\}$. We will show that if $L(\lambda)$ has a nonzero W -invariant bilinear product \cdot , then $p = 7$ and $\lambda = 3$.

By step (i), we may assume that $m_0 \cdot m_{p-1} = m_\lambda$. For $k \in \{1, \dots, p-2\}$,

$$\begin{aligned} (\lambda+1)(k+1)m_k \cdot m_{p-1} &= e_k(m_0) \cdot m_{p-1} \\ &= e_k(m_0 \cdot m_{p-1}) = e_k(m_\lambda) \\ &= (\lambda + (\lambda+1)(k+1))m_{\lambda+k}, \end{aligned}$$

so

$$m_k \cdot m_{p-1} = \frac{(\lambda+1)(k+1) + \lambda}{(\lambda+1)(k+1)} m_{\lambda+k}, \quad (14)$$

for $k \in \{1, \dots, p-2\}$. On the other hand, $e_1(e_1(m_\lambda)) = e_1(e_1(m_0) \cdot m_{p-1})$, and this gives

$$3(3\lambda+2)(\lambda+1)m_{\lambda+2} = 2(\lambda+1)(2\lambda+3)m_2 \cdot m_{p-1}. \quad (15)$$

If $2\lambda+3 = 0$, (15) gives $3\lambda+2 = 0$, and this implies $p = 5$ and $\lambda = 1$. But then, using (14) we get $e_1(m_2 \cdot m_4) = 2e_1(m_3) = 4m_4$, while at the same time

$$e_1(m_2 \cdot m_4) = (e_1 m_3) \cdot m_4 + m_3 \cdot (e_1 m_4) = m_3 \cdot m_4 = -2m_4,$$

which is a contradiction.

Hence, we assume for the rest of the proof $2\lambda+3 \neq 0$. By (15), we have

$$m_2 \cdot m_6 = \frac{3(3\lambda+2)}{2(2\lambda+3)} m_{\lambda+2}.$$

Comparing this with (14) with $k = 2$ we obtain

$$\frac{3(3\lambda+2)}{2(2\lambda+3)} = \frac{4\lambda+3}{3(\lambda+1)}, \text{ so } \lambda(11\lambda+9) = 0.$$

If $p = 11$, the above relation implies that $\lambda = 0$, which is a contradiction with our choice of λ , so no invariant bilinear product exists for $p = 11$.

For the rest of the proof, assume that $p \neq 11$ and hence $\lambda = -\frac{9}{11}$. Now, from $e_1(e_1(e_1(m_\lambda))) = e_1(e_1(e_1(m_0) \cdot m_{p-1}))$, we obtain

$$(3\lambda+2)(3\lambda+3)(3\lambda+4)m_{\lambda+3} = (2\lambda+2)(2\lambda+3)(2\lambda+4)m_3 \cdot m_{p-1}.$$

Thus,

$$m_3 \cdot m_{p-1} = \frac{3(3\lambda+2)(3\lambda+4)}{4(2\lambda+3)(\lambda+2)} m_{\lambda+3}.$$

Comparing this with (14) for $k = 3$ we obtain

$$\frac{3(3\lambda+2)(3\lambda+4)}{(2\lambda+3)(\lambda+2)} = \frac{5\lambda+4}{(\lambda+1)}.$$

Hence,

$$17\lambda^2 + 38\lambda + 20 = 0.$$

Substituting $\lambda = -\frac{9}{11}$ in this relation we obtain that $p \mid 35$, so either $p = 7$ or $p = 5$. If $p = 5$, then $\lambda = -\frac{9}{11} = 1$, and it was shown above that no nonzero invariant bilinear product exists in this case. If $p = 7$, then $\lambda = -\frac{9}{11} = 3$. This completes the proof. \square

Remark 5. Let V and U be two irreducible modules for a Lie algebra \mathcal{L} over an arbitrary field \mathbb{F} , and let \mathbb{F}_{alg} be an algebraic closure of \mathbb{F} . Suppose that $V \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}$ and $U \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}$ are isomorphic as modules for $\mathcal{L} \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}$; then, V and U are isomorphic as modules for \mathcal{L} . Indeed, if $V \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}$ and $U \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}$ are isomorphic, then $\text{Hom}_{\mathcal{L}}(V, U) \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}} \cong \text{Hom}_{\mathcal{L} \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}}(V \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}, U \otimes_{\mathbb{F}} \mathbb{F}_{\text{alg}}) \neq 0$, so $\text{Hom}_{\mathcal{L}}(V, U) \neq 0$. The result follows since, by irreducibility, any nonzero \mathcal{L} -module homomorphism

from V to U is an \mathcal{L} -module isomorphism. In particular, this implies that, even when the ground field is not algebraically closed, Theorem 4 applies to modules for the Witt algebra that are absolutely irreducible (i.e., they remain irreducible after extending scalars to an algebraic closure).

2.3. Embeddings of W_1 and its twisted forms into G_2 . It is shown in [Pre83, HSpr] that, over an algebraically closed field of characteristic 7, the simple Lie algebra of type G_2 contains a unique conjugacy class of subalgebras isomorphic to the Witt algebra. With our results above, a different proof may be given, valid for not necessarily algebraically closed fields.

Theorem 6. *Let \mathbb{F} be an arbitrary field of characteristic 7. Then any two subalgebras S_1 and S_2 of $\text{Der}(\mathcal{C}_s)$ isomorphic to the Witt algebra are conjugate: there is an automorphism φ of \mathcal{C}_s such that $S_2 = \varphi S_1 \varphi^{-1}$.*

Proof. Let $S := \text{span}\{e_i : -1 \leq i \leq 5\}$ be the subalgebra of $\mathfrak{g} := \text{Der}(\mathcal{C}_s)$ isomorphic to the Witt algebra given by equations (6) and (11), and let \tilde{S} be an arbitrary subalgebra of \mathfrak{g} isomorphic to the Witt algebra. Take a basis $\{\tilde{e}_i : -1 \leq i \leq 5\}$ of \tilde{S} with $[\tilde{e}_i, \tilde{e}_j] = (j - i)\tilde{e}_{i+j}$. We will follow several steps:

- (i) \tilde{S} is a maximal subalgebra of \mathfrak{g} .

Proof. Since the Witt algebra does not admit nonsingular invariant bilinear forms (see, e.g. [Far86, Theorem 4.2]), the restriction of the Killing form κ of \mathfrak{g} to \tilde{S} is trivial; hence, by dimension count, \mathfrak{g}/\tilde{S} is isomorphic, as a module for \tilde{S} , to the dual of the adjoint module for \tilde{S} . In particular, \mathfrak{g}/\tilde{S} is an irreducible module for \tilde{S} , and this shows the maximality of \tilde{S} . \square

- (ii) The representation of \tilde{S} on \mathcal{C}_s^0 , the subspace of trace zero elements of \mathcal{C}_s , is restricted and absolutely irreducible.

Proof. As \tilde{S} is an ideal in its p -closure in \mathfrak{g} , step (i) implies that \tilde{S} is a restricted subalgebra of \mathfrak{g} , and hence, the corresponding representation of \tilde{S} on \mathcal{C}_s^0 is restricted.

In order to prove the second part, we may assume that \mathbb{F} is algebraically closed. Recall that the possible dimensions of restricted irreducible representations of the Witt algebra are 1, 6 and 7. Suppose that \mathcal{C}_s^0 has a one-dimensional trivial \tilde{S} -submodule X . The space X may be either non-degenerate or totally isotropic with respect to the symmetric bilinear form b_q of \mathcal{C}_s .

If $X = \mathbb{F}x$ is nondegenerate, then $q(x) \neq 0$ and $b_q(x, 1) = 0$. By (1), $\mathbb{F}1 \oplus X$ is a two-dimensional composition subalgebra of \mathcal{C}_s , so it is isomorphic to $\mathbb{F}p_1 \oplus \mathbb{F}p_2$ (with p_i as in Table 1). Now, by [SV00, Corollary 1.7.3], the isomorphism $\mathbb{F}1 \oplus \mathbb{F}x \cong \mathbb{F}p_1 \oplus \mathbb{F}p_2$ may be extended to an automorphism of \mathcal{C}_s . As \tilde{S} annihilates $\mathbb{F}1 \oplus \mathbb{F}x$, and the subalgebra of the derivations that annihilate $\mathbb{F}p_1 \oplus \mathbb{F}p_2$ is isomorphic to $\mathfrak{sl}_3(\mathbb{F})$ ([EK13, Proposition 4.29]), we obtain that the Witt algebra embeds into $\mathfrak{sl}_3(\mathbb{F})$, which is impossible.

If X is totally isotropic, then $X \subseteq X^\perp$, and X^\perp/X is a 5-dimensional module for \tilde{S} . As this cannot be irreducible, we deduce that all the composition factors of \mathcal{C}_s^0 are one-dimensional. Hence, the representation ρ of \tilde{S} on \mathcal{C}_s^0 is nilpotent. Since $\text{ad}_{(\tilde{e}_0 + \tilde{e}_i)}$ is diagonalizable for $i \neq 0$, $-1 \leq i \leq 5$, then $\text{ad}_{(\tilde{e}_0 + \tilde{e}_i)}^p = \text{ad}_{(\tilde{e}_0 + \tilde{e}_i)}$. As the representation of \tilde{S} on \mathcal{C}_s^0 is restricted, then $\rho(\tilde{e}_0 + \tilde{e}_i)^p = \rho(\tilde{e}_0 + \tilde{e}_i)$, and the nilpotency implies that $\rho(\tilde{e}_0 + \tilde{e}_i) = 0$, for any $i \neq 0$, $-1 \leq i \leq 5$. This is a contradiction.

Finally, if Y is a 6-dimensional irreducible \tilde{S} -submodule for \mathcal{C}_s^0 , then it must be nondegenerate with respect to b_q . This implies that Y^\perp is a one-dimensional nondegenerate submodule, and we may use the above argument with $X = Y^\perp$. \square

- (iii) Note that \mathcal{C}_s^0 is not the adjoint module for \tilde{S} because of the existence of the invariant bilinear form b_q on \mathcal{C}_s^0 .
- (iv) The previous steps together with Theorem 4 and Remark 5 imply that, even when \mathbb{F} is not algebraically closed, there is a unique possibility, up to isomorphism, for \mathcal{C}_s^0 as a module for \tilde{S} , and a unique, up to scalars, nonzero \tilde{S} -invariant product on \mathcal{C}_s^0 . Therefore, there is a basis $\{\tilde{m}_i : 0 \leq i \leq 6\}$ of \mathcal{C}_s^0 with

$$\tilde{e}_k(\tilde{m}_i) = \begin{cases} (i + 4k + 4)\tilde{m}_{i+k} & \text{if } i + k \geq 6, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\frac{1}{2}[\tilde{m}_i \tilde{m}_j] = c(i, j)\tilde{m}_{i+j-3}$$

for $-1 \leq k \leq 5$ and $0 \leq i, j \leq 6$. Since the multiplication on a Cayley algebra is determined by the bracket of trace zero elements, the linear map φ that takes 1 to 1 and m_i to \tilde{m}_i , for $i \in \{0, \dots, 6\}$, is an automorphism of \mathcal{C}_s such that $\tilde{S} = \varphi S \varphi^{-1}$. \square

To finish this section, note that the Witt algebra W over a field \mathbb{F} of characteristic 7 is equal to the Lie algebra $\mathbb{F}[X]/(X^7) = \mathbb{F}[Z]/(Z^7 - 1)$, where $Z = X + 1$. Denote by z the class of Z modulo $(Z^7 - 1) = ((Z - 1)^7)$. The elements $f_i = z^{i+1} \frac{\partial}{\partial z}$, for $i \in \{-1, 0, \dots, 5\}$, form a basis of W with

$$[f_i, f_j] = (j - i)f_{i+j}, \quad (16)$$

where, contrary to (13), the indices are taken modulo 7. Now we may define an action of W on V_6 by changing slightly the definition in (11):

$$f_k(m_i) = (i + 4k + 4)m_{i+k}, \quad (17)$$

for $-1 \leq k \leq 5$ and $0 \leq i \leq 6$, with indices taken modulo 7. This gives another representation of W on V_6 :

$$\begin{aligned} f_r(f_s(m_i)) - f_s(f_r(m_i)) &= \left((i + s + 4r + 4)(i + 4s + 4) - (i + r + 4s + 4)(i + 4r + 4) \right) m_{i+s+r} \\ &= (s - r)(i + 4(r + s) + 4)m_{i+s+r} \\ &= [f_r, f_s](m_i). \end{aligned}$$

Equation (8) proves that this is a representation by derivations, so W embeds in $\text{Der}(V_6, \cdot)$, and hence on $\text{Der}(\mathcal{C}_s)$ as well. This embedding is different from the one obtained through (11), but Theorem 6 shows that they are conjugate.

We may even go a step further. For any $0 \neq \alpha \in \mathbb{F}$, consider the Lie algebra $W^\alpha = \text{Der}(\mathbb{F}[Y]/(Y^7 - \alpha))$, and denote by y the class of Y modulo $(Y^7 - \alpha)$. For any natural number i , consider the element $\tilde{f}_i = y^{i+1} \frac{\partial}{\partial y}$ in W^α , so $\{\tilde{f}_i : -1 \leq i \leq 5\}$ is a basis of W^α , and $\tilde{f}_{i+7} = \alpha \tilde{f}_i$ for any i . Define $m_{i+7} := \alpha m_i$. For $0 \leq i, j \leq 6$, $c(i, j) = 0$ if $i + j - 3 > 6$ or $i + j - 3 < 0$, so if we modify (17) as follows:

$$\tilde{f}_k(m_i) = (i + 4k + 4)m_{i+j-3}, \quad (18)$$

for any i, k (but now $\tilde{f}_{k+7} = \alpha \tilde{f}_k$ and $m_{i+7} = \alpha m_i$). The same computations as above show that W^α embeds in $\text{Der}(\mathcal{C}_s)$.

The twisted forms of the Witt algebra are precisely the algebras W^α ; if $0 \neq \alpha \in \mathbb{F}^7$, W^α is isomorphic to the Witt algebra, while if $\alpha \in \mathbb{F} \setminus \mathbb{F}^7$, W^α is the Lie algebra of derivations of the purely inseparable field extension $\mathbb{F}[Y]/(Y^7 - \alpha)$. Two algebras W^α and W^β are isomorphic if and only if so are the algebras $\mathbb{F}[Y]/(Y^7 - \alpha)$ and $\mathbb{F}[Y]/(Y^7 - \beta)$. (See [AS69] or [Wat71].)

Therefore, Theorems 2 and 6 may be extended as follows:

Theorem 7. *Over a field of characteristic 7, all the twisted forms of the Witt algebra embed in the Lie algebra of derivations of the split Cayley algebra. Moreover, any two embeddings of the same twisted form of the Witt algebra in $\text{Der}(\mathcal{C}_s)$ are conjugate.*

The last part of this theorem follows by the same arguments as in the proof of Theorem 6.

Remark 8. If \mathcal{C} is a non split Cayley algebra (and hence it is a division algebra, since q is anisotropic), then $\text{Der}(\mathcal{C})$ contains no nonzero nilpotent derivation. Indeed, if $d \in \text{Der}(\mathcal{C})$ is nilpotent, then $\ker d|_{\mathcal{C}^0}$ is a subspace of \mathcal{C}^0 and, since q is anisotropic, $\mathcal{C}^0 = \ker d|_{\mathcal{C}^0} \oplus (\ker d|_{\mathcal{C}^0})^\perp$. Besides, since q is invariant under the action of d (because of (1)), d leaves $(\ker d|_{\mathcal{C}^0})^\perp$ invariant; this is a contradiction because the nilpotency of d implies that any nonzero invariant subspace has nontrivial intersection with the kernel.

Therefore, $\text{Der}(\mathcal{C})$ cannot contain subalgebras isomorphic to twisted forms of the Witt algebra, because these algebras contain nilpotent elements. (Recall that the action of the Witt algebra on \mathcal{C}_s^0 is restricted, and hence so is the action on \mathcal{C}^0 of any subalgebra of $\text{Der}(\mathcal{C})$ isomorphic to a twisted form of the Witt algebra.)

3. CHARACTERISTIC 3

Let \mathcal{C} be a Cayley algebra over a field \mathbb{F} of characteristic $p \neq 2$. Then, the subspace of trace zero elements \mathcal{C}^0 is closed under the commutator $[\cdot, \cdot]$, and it satisfies (3). The anticommutative algebra $(\mathcal{C}^0, [\cdot, \cdot])$ is a central simple Malcev algebra. If $p \neq 2, 3$, any central simple non Lie Malcev algebra is isomorphic to one of these. However, if $p = 3$, then \mathcal{C}^0 is a simple Lie algebra; more precisely, it is a twisted form of the projective special linear Lie algebra $\mathfrak{psl}_3(\mathbb{F})$, and any such twisted form is obtained, up to isomorphism, in this way. (See [AEMN02] or [EK13, Theorem 4.26].)

Denote by $\mathbf{Aut}(\mathcal{A})$ the affine group scheme of automorphisms of a finite-dimensional algebra \mathcal{A} . Equations (2) and (3) show that the restriction map

$$\begin{aligned} \mathbf{Aut}(\mathcal{C}) &\longrightarrow \mathbf{Aut}(\mathcal{C}^0) \\ f &\longmapsto f|_{\mathcal{C}^0}, \end{aligned} \tag{19}$$

gives an isomorphism of group schemes. (The reader may consult [KMRT98, Chapter VI] for the basic facts of affine group schemes.)

For the rest of this section, assume that \mathcal{C} is a Cayley algebra over a field \mathbb{F} of characteristic 3, and write $\mathfrak{g} := \text{Der}(\mathcal{C})$. Any derivation $d \in \mathfrak{g}$ satisfies $d(1) = 0$ and $d(\mathcal{C}^0) \subseteq \mathcal{C}^0$, and hence, because of (2) and (3), we may identify \mathfrak{g} with $\text{Der}(\mathcal{C}^0)$. Since \mathcal{C}^0 is a Lie algebra, $\text{ad}_{\mathcal{C}^0}$ is an ideal of \mathfrak{g} : the ideal of inner derivations. In fact, $\text{ad}_{\mathcal{C}^0}$ is the only proper ideal of \mathfrak{g} , and the quotient $\mathfrak{g}/\text{ad}_{\mathcal{C}^0}$ is again isomorphic to $\mathcal{C}^0 \cong \text{ad}_{\mathcal{C}^0}$ (see [AEMN02]).

In the split case, $\text{ad}_{\mathcal{C}_s^0}$ is the ideal of the Chevalley algebra of type G_2 generated by the root spaces corresponding to the short roots (see [Ste68, p. 156]).

Lemma 9. *Any derivation of $\mathfrak{g} := \text{Der}(\mathcal{C})$ is inner.*

Proof. Let $d \in \text{Der}(\mathfrak{g})$ and let $\mathfrak{i} = \text{ad}_{\mathcal{C}^0}$ be the unique proper ideal of \mathfrak{g} . The ideal \mathfrak{i} is simple, so $\mathfrak{i} = [\mathfrak{i}, \mathfrak{i}]$, and hence $d(\mathfrak{i}) \subseteq [d(\mathfrak{i}), \mathfrak{i}] \subseteq \mathfrak{i}$, so $d|_{\mathfrak{i}}$ is a derivation of $\mathfrak{i} = \text{ad}_{\mathcal{C}^0} \cong \mathcal{C}^0$. Since any derivation δ of \mathcal{C}^0 extends to a derivation of \mathcal{C} by means of $\delta(1) = 0$, it follows that there exists a $\delta \in \mathfrak{g}$ such that $d|_{\mathfrak{i}} = \text{ad}_{\delta}|_{\mathfrak{i}}$. That is, $d(f) = [\delta, f]$ for any $f \in \mathfrak{i} = \text{ad}_{\mathcal{C}^0}$, so the derivation $\tilde{d} = d - \text{ad}_{\delta}$ satisfies $\tilde{d}(\mathfrak{i}) = 0$.

But if \tilde{d} is a derivation of \mathfrak{g} such that $\tilde{d}(\mathfrak{i}) = 0$, then $[\tilde{d}(\mathfrak{g}), \mathfrak{i}] \subseteq \tilde{d}([\mathfrak{g}, \mathfrak{i}] + [\mathfrak{g}, \tilde{d}(\mathfrak{i})]) = 0$, so $\tilde{d}(\mathfrak{g})$ is contained in the centralizer of \mathfrak{i} in \mathfrak{g} , which is trivial. In particular, the derivation $\tilde{d} = d - \text{ad}_{\delta}$ above is trivial, and hence $d = \text{ad}_{\delta}$ is inner. \square

Theorem 10. *Let \mathcal{C} be a Cayley algebra over a field \mathbb{F} of characteristic 3, and let $\mathfrak{g} := \text{Der}(\mathcal{C})$ be its Lie algebra of derivations. The the adjoint map*

$$\begin{aligned} \text{Ad} : \mathbf{Aut}(\mathcal{C}) &\longrightarrow \mathbf{Aut}(\mathfrak{g}) \\ f &\mapsto \varphi(f) : d \mapsto fdf^{-1}, \end{aligned}$$

is an isomorphism of affine group schemes.

Proof. Let \mathbb{F}_{alg} be an algebraic closure of \mathbb{F} . The group homomorphism $\text{Ad}_{\mathbb{F}_{\text{alg}}} : \mathbf{Aut}(\mathcal{C}_{\mathbb{F}_{\text{alg}}}) \rightarrow \text{Der}(\mathcal{C}_{\mathbb{F}_{\text{alg}}})$ is injective, where $\mathcal{C}_R = \mathcal{C} \otimes_{\mathbb{F}} R$, for any unital commutative and associative algebra R over \mathbb{F} . This is because $f \text{ad}_x f^{-1} = \text{ad}_{f(x)}$ for any $x \in \mathcal{C}_{\mathbb{F}_{\text{alg}}}^0$ and $f \in \mathbf{Aut}(\mathcal{C}_{\mathbb{F}_{\text{alg}}})$, so $\text{Ad}_{\mathbb{F}_{\text{alg}}}(f) = \text{id}$ implies $f|_{\mathcal{C}_{\mathbb{F}_{\text{alg}}}^0} = \text{id}$; hence, $f = \text{id}$.

As any $\varphi \in \mathbf{Aut}(\mathfrak{g}_{\mathbb{F}_{\text{alg}}})$ preserves the only proper ideal $\mathfrak{i}_{\mathbb{F}_{\text{alg}}} = \text{ad}_{\mathcal{C}_{\mathbb{F}_{\text{alg}}}^0}$, the automorphism φ induces an automorphism f of $\mathcal{C}_{\mathbb{F}_{\text{alg}}}^0$, which extends to an automorphism of $\mathcal{C}_{\mathbb{F}_{\text{alg}}}$ also denoted by f . Then $\varphi \text{Ad}(f)^{-1}|_{\mathfrak{i}_{\mathbb{F}_{\text{alg}}}} = \text{id}$, and, as in the proof above, a simple argument gives $\varphi \text{Ad}(f)^{-1} = \text{id}$, so $\varphi = \text{Ad}(f)$. This shows that $\text{Ad}_{\mathbb{F}_{\text{alg}}}$ is a bijection.

But it also shows that $\dim \mathbf{Aut}(\mathfrak{g}) = \dim \mathbf{Aut}(\mathcal{C})$ and, since this latter group scheme is smooth (this follows from [SV00, Proposition 2.2.3], see also [EK13, Proof of Theorem 4.35]), we obtain $\dim \mathbf{Aut}(\mathfrak{g}) = \dim \text{Der}(\mathcal{C}) = \dim \text{Der}(\mathfrak{g})$ by Lemma 9. Therefore, $\mathbf{Aut}(\mathfrak{g})$ is smooth.

Since the differential map $d(\text{Ad}) : \text{Der}(\mathcal{C}) \rightarrow \text{Der}(\mathfrak{g})$, $\delta \mapsto \text{ad}_{\delta}$, is injective, [KMRT98, (22.5)] shows that Ad is an isomorphism. \square

Denote by $\text{Isom}(\text{Cayley})$, $\text{Isom}(G_2)$, and $\text{Isom}(\bar{A}_2)$, the sets of isomorphism classes of Cayley algebras, twisted forms of the Chevalley algebra of type G_2 , and twisted forms of $\mathfrak{psl}_3(\mathbb{F})$, respectively. Theorem 10 and (19) immediately give the following consequence, where $[A]$ denotes the isomorphism class of the algebra A .

Corollary 11. *The maps $[\mathcal{C}] \mapsto [\text{Der}(\mathcal{C})]$ and $[\mathcal{C}] \mapsto [\mathcal{C}^0]$ give bijections $\text{Isom}(\text{Cayley}) \rightarrow \text{Isom}(G_2)$ and $\text{Isom}(\text{Cayley}) \rightarrow \text{Isom}(\bar{A}_2)$, respectively.*

4. CHARACTERISTIC 2

In this section, assume that the characteristic of the ground field \mathbb{F} is 2. In [EK13, Corollary 4.32] it is proved that the Chevalley algebra of type G_2 (i.e., the Lie algebra $\text{Der}(\mathcal{C}_s)$), is isomorphic to the projective special linear Lie algebra $\mathfrak{psl}_4(\mathbb{F})$. Here we extend this result for the Lie algebra of derivations of any Cayley algebra over \mathbb{F} .

Let V be a finite-dimensional vector space over \mathbb{F} , and let b be a nondegenerate alternating (i.e., $b(u, u) = 0$ for any $u \in V$) bilinear form of V . Denote by $\mathfrak{sp}(V, b)$ the corresponding symplectic Lie algebra:

$$\mathfrak{sp}(V, b) = \{f \in \mathfrak{gl}(V) : b(f(u), v) + b(u, f(v)) = 0 \ \forall u, v \in V\}.$$

In particular, $\mathfrak{sp}_{2n}(\mathbb{F})$ denotes the symplectic Lie algebra $\mathfrak{sp}(\mathbb{F}^{2n}, b_s)$, where b_s is the alternating bilinear form with coordinate matrix $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ in the canonical basis. (Notice that, as $\text{char}(\mathbb{F}) = 2$, there is no need of minus signs.) We identify the elements of $\mathfrak{sp}_{2n}(\mathbb{F})$ with their coordinate matrices in the canonical basis.

A matrix in $M_n(\mathbb{F})$ is called *alternating* if it has the form $a + a^t$ for some $a \in M_n(\mathbb{F})$, where a^t denotes the transpose of a . These are the coordinate matrices of the alternating bilinear forms.

Lemma 12. *The second derived power of the symplectic Lie algebra on a vector space of dimension 6 is isomorphic to the projective special linear Lie algebra $\mathfrak{psl}_4(\mathbb{F})$:*

$$\mathfrak{sp}_6(\mathbb{F})^{(2)} \cong \mathfrak{psl}_4(\mathbb{F}).$$

Proof. For any natural number n we have

$$\mathfrak{sp}_{2n}(\mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ c & a^t \end{pmatrix} : a, b, c \in M_n(\mathbb{F}), \ b^t = b, \ c^t = c \right\}.$$

A direct computation gives

$$\begin{aligned} \mathfrak{sp}_{2n}(\mathbb{F})^{(1)} &= \left\{ \begin{pmatrix} a & b \\ c & a^t \end{pmatrix} : a, b, c \in M_n(\mathbb{F}), \ b \text{ and } c \text{ alternating} \right\}, \\ \mathfrak{sp}_{2n}(\mathbb{F})^{(2)} &= \left\{ \begin{pmatrix} a & b \\ c & a^t \end{pmatrix} : a, b, c \in M_n(\mathbb{F}), \ a \in \mathfrak{sl}_n(\mathbb{F}), \ b \text{ and } c \text{ alternating} \right\}. \end{aligned}$$

The dimension of $\mathfrak{sp}_{2n}(\mathbb{F})^{(2)}$ is then $n^2 - 1 + 2\binom{n}{2} = 2n^2 - n - 1$.

Let V be a four-dimensional vector space, and consider the second exterior power $\bigwedge^2 V$ as a module for $\mathfrak{sl}(V)$. Fix a nonzero linear isomorphism $\det : \bigwedge^4 V \rightarrow \mathbb{F}$ and define the nondegenerate alternating bilinear form

$$\begin{aligned} b : \bigwedge^2 V \times \bigwedge^2 V &\longrightarrow \mathbb{F} \\ (u_1 \wedge u_2, v_1 \wedge v_2) &\mapsto \det(u_1 \wedge u_2 \wedge v_1 \wedge v_2). \end{aligned}$$

Then, the action of $\mathfrak{sl}(V)$ on $\bigwedge^2 V$ gives a Lie algebra homomorphism

$$\Phi : \mathfrak{sl}(V) \rightarrow \mathfrak{sp}(\bigwedge^2 V, b) \cong \mathfrak{sp}_6(\mathbb{F}),$$

with kernel $\mathbb{F}I_V$ (where I_V denotes the identity map on V), so Φ induces an injection $\mathfrak{psl}(V) \hookrightarrow \mathfrak{sp}(\bigwedge^2 V, b)$. But $\mathfrak{psl}(V)$ is simple of dimension 14, so, in particular, $\mathfrak{psl}(V)^{(2)} = \mathfrak{psl}(V)$, and the dimension of $\mathfrak{sp}(\bigwedge^2 V, b)^{(2)} \cong \mathfrak{sp}_6(\mathbb{F})^{(2)}$ is $2 \times 3^2 - 3 - 1 = 14$. Therefore, Φ induces an isomorphism $\mathfrak{psl}(V) \cong \mathfrak{sp}(\bigwedge^2 V, b)^{(2)}$, as required. \square

We will need some extra notation. As above, let (V, b) be a finite-dimensional vector space endowed with a nondegenerate alternating bilinear form. Denote by $\mathfrak{gsp}(V, b)$ the Lie algebra of the group of similarities (i.e., the general symplectic Lie algebra):

$$\begin{aligned} \mathfrak{gsp}(V, b) &= \{f \in \mathfrak{gl}(V) : \exists \lambda \in \mathbb{F} \text{ such that} \\ &\quad b(f(u), v) + b(u, f(v)) = \lambda b(u, v) \ \forall u, v \in V\}, \end{aligned}$$

and by $\mathfrak{pgsp}(V, b)$ the projective general symplectic Lie algebra (i.e., the quotient of $\mathfrak{gsp}(V, b)$ by the one-dimensional ideal generated by I_V). In particular, after choosing a basis, we get the Lie algebras $\mathfrak{gsp}_{2n}(\mathbb{F})$ and $\mathfrak{pgsp}_{2n}(\mathbb{F})$.

Corollary 13. *The Lie algebra of derivations of $\mathfrak{psl}_4(\mathbb{F})$ is isomorphic to the projective general symplectic Lie algebra $\mathfrak{pgsp}_6(\mathbb{F})$:*

$$\text{Der}(\mathfrak{psl}_4(\mathbb{F})) \cong \mathfrak{pgsp}_6(\mathbb{F}).$$

Proof. Note that we have the decomposition

$$\mathfrak{gsp}_6(\mathbb{F}) = \mathfrak{sp}_6(\mathbb{F}) \oplus \mathbb{F} \begin{pmatrix} I_3 & 0 \\ 0 & 0 \end{pmatrix},$$

and one may easily check that $\mathfrak{gsp}_6(\mathbb{F})^{(1)} = \mathfrak{sp}_6(\mathbb{F})$.

For any $A \in \mathfrak{gsp}_6(\mathbb{F})$, $\text{ad}_A : B \mapsto [A, B]$ leaves invariant $\mathfrak{gsp}_6(\mathbb{F})^{(3)} = \mathfrak{sp}_6(\mathbb{F})^{(2)}$, which is isomorphic to $\mathfrak{psl}_4(\mathbb{F})$ by Lemma 12, so we obtain a Lie algebra homomorphism

$$\begin{aligned} \Phi : \mathfrak{gsp}_6(\mathbb{F}) &\longrightarrow \text{Der}(\mathfrak{sp}_6(\mathbb{F})^{(2)}) \left(\cong \text{Der}(\mathfrak{psl}_4(\mathbb{F})) \right), \\ A &\mapsto \text{ad}_A|_{\mathfrak{sp}_6(\mathbb{F})^{(2)}}. \end{aligned}$$

The kernel of Φ is the centralizer in $\mathfrak{gsp}_6(\mathbb{F})$ of $\mathfrak{sp}_6(\mathbb{F})^{(2)}$, which is $\mathbb{F}I_6$, so Φ induces an injection $\mathfrak{pgsp}_6(\mathbb{F}) \rightarrow \text{Der}(\mathfrak{psl}_4(\mathbb{F}))$. The dimension of $\mathfrak{pgsp}_6(\mathbb{F})$ is 21, and (as it may be calculated in GAP as in [AMMpr]) this is also the dimension of $\text{Der}(\mathfrak{psl}_4(\mathbb{F}))$. The result follows. \square

In fact, in order to prove the previous result, the exact computation of the dimension of $\text{Der}(\mathfrak{psl}_4(\mathbb{F}))$ is not required; we just need the bound

$$\dim \text{Der}(\mathfrak{psl}_4(\mathbb{F})) \leq 21.$$

For completeness, let us provide an elementary proof of this fact.

Lemma 14. $\dim \text{Der}(\mathfrak{psl}_4(\mathbb{F})) \leq 21$.

Proof. For $1 \leq i, j \leq 4$, let E_{ij} be the matrix in $\mathfrak{gl}_4(\mathbb{F})$ with 1 in the (i, j) entry and 0's elsewhere. Denote by \bar{A} the class of a matrix $A \in \mathfrak{sl}_4(\mathbb{F})$ in $\mathfrak{psl}_4(\mathbb{F})$.

Then, $\mathfrak{sl}_4(\mathbb{F})$ is graded by \mathbb{Z}^3 , with

$$\begin{aligned} \text{degree}(E_{12}) &= (1, 0, 0) = -\text{degree}(E_{21}), \\ \text{degree}(E_{23}) &= (0, 1, 0) = -\text{degree}(E_{32}), \\ \text{degree}(E_{34}) &= (0, 0, 1) = -\text{degree}(E_{43}). \end{aligned}$$

As the identity matrix I_4 is homogeneous of degree $(0, 0, 0)$, this induces a grading by \mathbb{Z}^3 on $\mathfrak{g} = \mathfrak{psl}_4(\mathbb{F})$:

$$\Gamma : \mathfrak{g} = \bigoplus_{\alpha \in \mathbb{Z}^3} \mathfrak{g}_\alpha,$$

with support

$$\begin{aligned} \text{Supp } \Gamma &:= \{\alpha \in \mathbb{Z}^3 : \mathfrak{g}_\alpha \neq 0\} \\ &= \{(0, 0, 0), \pm(1, 0, 0), \pm(0, 1, 0), \pm(0, 0, 1), \pm(1, 1, 0), \pm(0, 1, 1), \pm(1, 1, 1)\}. \end{aligned}$$

Let $\mathfrak{h} = \text{span}\{H_1 := \overline{E_{11} + E_{22}}, H_2 := \overline{E_{22} + E_{33}}\} = \mathfrak{g}_{(0,0,0)}$ be the ‘diagonal’ subalgebra of \mathfrak{g} . Then, the decomposition in eigenspaces for the adjoint action of \mathfrak{h} is $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \mathfrak{g}_3$, with

$$\begin{aligned} \mathfrak{g}_1 &= \text{span}\{\bar{E}_{12}, \bar{E}_{21}, \bar{E}_{34}, \bar{E}_{43}\} = \mathfrak{g}_{(1,0,0)} \oplus \mathfrak{g}_{(-1,0,0)} \oplus \mathfrak{g}_{(0,0,1)} \oplus \mathfrak{g}_{(0,0,-1)}, \\ \mathfrak{g}_2 &= \text{span}\{\bar{E}_{23}, \bar{E}_{32}, \bar{E}_{14}, \bar{E}_{41}\} = \mathfrak{g}_{(0,1,0)} \oplus \mathfrak{g}_{(0,-1,0)} \oplus \mathfrak{g}_{(1,1,1)} \oplus \mathfrak{g}_{(-1,-1,-1)}, \\ \mathfrak{g}_3 &= \text{span}\{\bar{E}_{13}, \bar{E}_{31}, \bar{E}_{24}, \bar{E}_{42}\} = \mathfrak{g}_{(1,1,0)} \oplus \mathfrak{g}_{(-1,-1,0)} \oplus \mathfrak{g}_{(0,1,1)} \oplus \mathfrak{g}_{(0,-1,-1)}. \end{aligned}$$

As \mathfrak{g} is \mathbb{Z}^3 -graded, so is $\text{Der}(\mathfrak{g})$. Several steps are required now:

- (i) $\dim \text{Der}(\mathfrak{g})_{(0,0,0)} \leq 3$, and $d(\mathfrak{h}) = 0$ for any $d \in \text{Der}(\mathfrak{g})_{(0,0,0)}$.

Proof. Any $d \in \text{Der}(\mathfrak{g})_{(0,0,0)}$ preserves the one-dimensional spaces \mathfrak{g}_α , for $\alpha \in \text{Supp } \Gamma \setminus \{(0, 0, 0)\}$. Then d and $\text{ad}_{\mathfrak{h}}$ commute, so $d(\mathfrak{h}) = 0$. Also $d(\bar{E}_{12}) = \lambda \bar{E}_{12}$ and $d(\bar{E}_{23}) = \mu \bar{E}_{23}$ for some $\lambda, \mu \in \mathbb{F}$. From $d(\mathfrak{h}) = 0$, we obtain that $d(\bar{E}_{21}) = -\lambda \bar{E}_{21}$ and $d(\bar{E}_{32}) = -\mu \bar{E}_{32}$. Hence $\tilde{d} := d -$

$\text{ad}_{\mu_{H_2} + \lambda_{H_1}}$ annihilates \bar{E}_{12} and \bar{E}_{23} (and \bar{E}_{21} and \bar{E}_{32}). Since the elements \bar{E}_{12} , \bar{E}_{21} , \bar{E}_{23} , \bar{E}_{32} , \bar{E}_{34} and \bar{E}_{43} generate \mathfrak{g} , it follows that \tilde{d} is determined by the value $\tilde{d}(E_{34})$. We conclude that $\dim \text{Der}(\mathfrak{g})_{(0,0,0)} - \dim \text{ad}_{\mathfrak{h}} \leq 1$. \square

- (ii) $\text{Der}(\mathfrak{g}) = \text{ad}_{\mathfrak{g}} + \{d \in \text{Der}(\mathfrak{g}) : d(\mathfrak{h}) = 0\}$.

Proof. We already have $\text{Der}(\mathfrak{g})_{(0,0,0)} \subseteq \{d \in \text{Der}(\mathfrak{g}) : d(\mathfrak{h}) = 0\}$, and it is clear that $d \in \text{Der}(\mathfrak{g})_{\alpha}$, with $\alpha \in \mathbb{Z}^3 \setminus \text{Supp } \Gamma$, implies $d(\mathfrak{h}) \subseteq \mathfrak{g}_{\alpha} = 0$. On the other hand, if $d \in \text{Der}(\mathfrak{g})_{\alpha}$, with $\alpha \in \text{Supp } \Gamma \setminus \{(0,0,0)\}$, then the restriction of d to \mathfrak{h} defines a linear map $\beta : \mathfrak{h} \rightarrow \mathbb{F}$ by $d(H) = \beta(H)\bar{E}_{rs}$, where \bar{E}_{rs} is the basic element in the one-dimensional space \mathfrak{g}_{α} . But for any $H, H' \in \mathfrak{h}$ we get:

$$\begin{aligned} 0 &= d([H, H']) = [d(H), H'] + [H, d(H')] \\ &= \beta(H)[\bar{E}_{rs}, H'] + \beta(H')[H, \bar{E}_{rs}] \\ &= (-\beta(H)\gamma(H') + \beta(H')\gamma(H))\bar{E}_{rs}, \end{aligned}$$

where $\gamma : \mathfrak{h} \rightarrow \mathbb{F}$ is the nonzero linear form such that $[H, \bar{E}_{rs}] = \gamma(H)\bar{E}_{rs}$ for any $H \in \mathfrak{h}$. Hence β is a scalar multiple of γ , and if $\beta = \nu\gamma$ with $\nu \in \mathbb{F}$, then $(d - \nu \text{ad}_{\bar{E}_{rs}})(\mathfrak{h}) = 0$. (This argument is similar to the one in [EK12, Proposition 8.1].) \square

- (iii) Now note that \bar{E}_{12} , \bar{E}_{23} , \bar{E}_{34} and \bar{E}_{41} generate \mathfrak{g} . Let $0 \neq d \in \text{Der}(\mathfrak{g})_{\alpha}$, with $\alpha \in \mathbb{Z}_3 \setminus \{(0,0,0)\}$, and $d(\mathfrak{h}) = 0$. Then $d(\mathfrak{g}_i) \subseteq \mathfrak{g}_i$, for $i = 1, 2, 3$, and $d(\bar{E}_{12}) \in \mathfrak{g}_1$ so either $d(\bar{E}_{12}) = 0$ or $\alpha \in \{(-2, 0, 0), (-1, 0, 1), (-1, 0, -1)\}$, $d(\bar{E}_{23}) \in \mathfrak{g}_2$ so either $d(\bar{E}_{23}) = 0$ or $\alpha \in \{(0, -2, 0), (1, 0, 1), (-1, -2, -1)\}$, $d(\bar{E}_{34}) \in \mathfrak{g}_1$ so either $d(\bar{E}_{34}) = 0$ or $\alpha \in \{(0, 0, -2), (1, 0, -1), (-1, 0, 1)\}$, $d(\bar{E}_{41}) \in \mathfrak{g}_2$ so either $d(\bar{E}_{41}) = 0$ or $\alpha \in \{(2, 2, 2), (1, 2, 1), (1, 0, -1)\}$.

But $\text{Der}(\mathfrak{g})_{\alpha} = 0$ for $\alpha \in \{(-2, 0, 0), (0, -2, 0), (0, 0, -2), (2, 2, 2)\}$, because any d in one of these homogeneous spaces annihilates the generators \bar{E}_{21} , \bar{E}_{32} , \bar{E}_{43} and \bar{E}_{14} . Hence, our homogeneous d belongs to $\text{Der}(\mathfrak{g})_{\alpha}$ with $\alpha \in X := \{\pm(1, 0, 1), \pm(1, 0, -1), \pm(1, 2, 1)\}$. Now if, for instance, $d \in \text{Der}(\mathfrak{g})_{(-1,0,-1)}$, then d annihilates $\bar{E}_{23} \in \mathfrak{g}_{(0,1,0)}$ (because $(0, 1, 0) + (-1, 0, -1) \notin \text{Supp } \Gamma$), $\bar{E}_{41} \in \mathfrak{g}_{(-1,-1,-1)}$, and $\bar{E}_{24} \in \mathfrak{g}_{(1,1,0)}$. Moreover, since $\bar{E}_{34} = [[\bar{E}_{31}, \bar{E}_{12}], \bar{E}_{24}]$, it follows that d is determined by the value $d(\bar{E}_{12})$. Thus, we get $\dim \text{Der}(\mathfrak{g})_{(-1,0,-1)} \leq 1$. A similar argument applies to the other possibilities, so $\dim \text{Der}(\mathfrak{g})_{\alpha} \leq 1$ for any $\alpha \in X$.

- (iv) Therefore, we conclude that

$$\dim \text{Der}(\mathfrak{g}) - \dim \mathfrak{g} = \left(\dim \text{Der}(\mathfrak{g})_{(0,0,0)} - \dim \mathfrak{h} \right) + \sum_{\alpha \in X} \dim \text{Der}(\mathfrak{g})_{\alpha} \leq 7,$$

so that $\dim \text{Der}(\mathfrak{g}) \leq \dim \mathfrak{g} + 7 = 21$. \square

Our next result extends [EK13, Corollary 4.32].

Theorem 15. *Let \mathcal{C} be a Cayley algebra over a field \mathbb{F} of characteristic 2. The Lie algebra of derivations $\text{Der}(\mathcal{C})$ is isomorphic to the projective special linear Lie algebra $\mathfrak{psl}_4(\mathbb{F})$. (Independently of the isomorphism class of \mathcal{C} !)*

Proof. Recall that $\text{Der}(\mathcal{C})$ is a 14-dimensional simple Lie algebra, a twisted form of $\text{Der}(\mathcal{C}_s)$, which is the Chevalley algebra of type G_2 .

Any $d \in \text{Der}(\mathcal{C})$ leaves the norm q invariant, annihilates the unity 1 and preserves \mathcal{C}^0 , the subspace of trace zero elements. Since the characteristic is 2, the unity 1 is in \mathcal{C}^0 , so d induces an element \tilde{d} in the symplectic Lie algebra $\mathfrak{sp}(\mathcal{C}^0/\mathbb{F}1, \tilde{b}_q) \cong \mathfrak{sp}_6(\mathbb{F})$,

where \tilde{b}_q is the nondegenerate alternating bilinear form on \mathcal{C}^0 induced by b_q . (Note that $\mathcal{C}^0 = \{x \in \mathcal{C} : b_q(x, 1) = 0\}$, so \tilde{b}_q is nondegenerate.)

Therefore, we have a homomorphism of Lie algebras

$$\begin{aligned} \Phi : \text{Der}(\mathcal{C}) &\longrightarrow \mathfrak{sp}(\mathcal{C}^0/\mathbb{F}1, \tilde{b}_q), \\ d &\longmapsto \tilde{d}. \end{aligned}$$

The simplicity of $\text{Der}(\mathcal{C})$ implies that Φ is injective, and hence

$$\Phi(\text{Der}(\mathcal{C})) = \Phi(\text{Der}(\mathcal{C})^{(2)}) \subseteq \mathfrak{sp}(\mathcal{C}^0/\mathbb{F}1, \tilde{b}_q)^{(2)} \cong \mathfrak{sp}_6(\mathbb{F})^{(2)}.$$

By dimension count, the image of Φ is $\mathfrak{sp}(\mathcal{C}^0/\mathbb{F}1, \tilde{b}_q)^{(2)}$, which is isomorphic to $\mathfrak{sp}_6(\mathbb{F})^{(2)}$, and hence to $\mathfrak{psl}_4(\mathbb{F})$ by Lemma 12. \square

The previous theorem shows that, in characteristic 2, it is no longer true that two Cayley algebras are isomorphic if and only if their Lie algebras of derivations are isomorphic.

Remark 16. Given an irreducible root system of type X_r and its corresponding Chevalley algebra \mathfrak{g} over a field \mathbb{F} , the quotient $\mathfrak{g}/Z(\mathfrak{g})$ (where $Z(\mathfrak{g})$ is the center of \mathfrak{g}) is usually called the *classical Lie algebra of type X_r* . In particular, in characteristic 2, Theorem 15 implies that the classical Lie algebras of type A_3 and G_2 coincide.

Write $\mathcal{A} := M_6(\mathbb{F})$, and let σ be the symplectic involution (attached to the standard alternating form b_s), such that, for any $X \in \mathcal{A}$, $\sigma(X)$ is the adjoint relative to b_s .

Theorem 17. *The affine group scheme of automorphisms of $\text{Der}(\mathcal{C}_s)$ is isomorphic to the affine group scheme of automorphisms of the algebra with involution (\mathcal{A}, σ) .*

Over an algebraic closure \mathbb{F}_{alg} , the group $\text{Aut}(\mathfrak{psl}_4(\mathbb{F}_{\text{alg}}))$ is the adjoint Chevalley group of type C_3 (see [Hog82]), and hence it is isomorphic to projective general symplectic group $\text{PGSp}_6(\mathbb{F}_{\text{alg}}) \cong \text{Aut}(\mathcal{A}, \sigma)$. However, Theorem 17 considers arbitrary fields, and we shall give an explicit isomorphism of schemes in its proof. Note that this result over \mathbb{F}_{alg} shows that $\mathbf{Aut}(\mathfrak{psl}_4(\mathbb{F}))$ is connected, and Corollary 4 shows that it is smooth.

Proof of Theorem 17. As in the proof of Theorem 15, we may identify $\text{Der}(\mathcal{C}_s) \cong \mathfrak{psl}_4(\mathbb{F})$ with the Lie algebra $\text{Skew}(\mathcal{A}, \sigma)^{(2)}$, where $\text{Skew}(\mathcal{A}, \sigma) := \{x \in \mathcal{A} : \sigma(x) = x\}$ (as the characteristic is two!) Consider the morphism of affine group schemes

$$\begin{aligned} \varphi : \mathbf{Aut}(\mathcal{A}, \sigma) &\longrightarrow \mathbf{Aut}\left(\text{Skew}(\mathcal{A}, \sigma)^{(2)}\right), \\ f : \mathcal{A}_R &\rightarrow \mathcal{A}_R \mapsto f|_{\text{Skew}(\mathcal{A}_R, \sigma_R)^{(2)}}, \end{aligned}$$

where R is a unital, commutative and associative \mathbb{F} -algebra, $\mathcal{A}_R = \mathcal{A} \otimes_{\mathbb{F}} R$, and $\sigma_R = \sigma \otimes \text{id}$ is the induced involution in \mathcal{A}_R , so $\text{Skew}(\mathcal{A}_R, \sigma_R)^{(2)} = \text{Skew}(\mathcal{A}, \sigma)^{(2)} \otimes_{\mathbb{F}} R$.

The group homomorphism on points in an algebraic closure \mathbb{F}_{alg}

$$\varphi_{\mathbb{F}_{\text{alg}}} : \text{Aut}(\mathcal{A}_{\mathbb{F}_{\text{alg}}}) \rightarrow \text{Aut}(\text{Skew}(\mathcal{A}_{\mathbb{F}_{\text{alg}}}, \sigma_{\mathbb{F}_{\text{alg}}})^{(2)})$$

is injective, because $\text{Skew}(\mathcal{A}_{\mathbb{F}_{\text{alg}}}, \sigma_{\mathbb{F}_{\text{alg}}})^{(2)} = \mathfrak{sp}_6(\mathbb{F}_{\text{alg}})^{(2)}$ generates $\mathcal{A}_{\mathbb{F}_{\text{alg}}} = M_6(\mathbb{F}_{\text{alg}})$ as an algebra. Also, the differential $d\varphi$ is an isomorphism: it is the isomorphism Φ in the proof of Corollary 4. Therefore, φ is a closed imbedding ([KMRT98, (22.2)]). But both schemes are smooth, connected, and of the same dimension, so φ is an isomorphism. \square

Since $\mathbf{Aut}(\mathfrak{psl}_4(\mathbb{F}))$ is smooth, the set of isomorphism classes of twisted forms of $\mathfrak{psl}_4(\mathbb{F})$ is in bijection with $H^1(\mathbb{F}, \mathbf{Aut}(\mathfrak{psl}_4(\mathbb{F})))$ (see [Wat79, Chapters 17 and 18]), and also the set of isomorphism classes of central simple associative algebras of degree 6 endowed with a symplectic involution is in bijection with $H^1(\mathbb{F}, \mathbf{Aut}(M_6(\mathbb{F}), \sigma) = H^1(\mathbb{F}, \mathrm{PGSp}_6(\mathbb{F})))$. Our last result is then a direct consequence of Theorem 17.

Corollary 18. *Let \mathbb{F} be a field of characteristic 2. The map that sends any central simple associative algebra of degree 6 over \mathbb{F} endowed with a symplectic involution (\mathcal{B}, τ) to the Lie algebra $\mathrm{Skew}(\mathcal{B}, \tau)^{(2)}$ gives a bijection between the set of isomorphism classes of such pairs (\mathcal{B}, τ) to the set of twisted forms over \mathbb{F} of the Lie algebra $\mathfrak{psl}_4(\mathbb{F})$.*

Recall that $\mathfrak{psl}_4(\mathbb{F})$ is (isomorphic to) the Chevalley algebra of type G_2 , so this corollary gives the twisted forms of the classical simple Lie algebras of type G_2 in characteristic 2.

REFERENCES

- [AEMN02] Bjerregaard, P. Alberca-Bjerregaard, A. Elduque, C. Martín-González, and F.J. Navarro-Márquez, *On the Cartan-Jacobson theorem*, J. Algebra **250** (2002), no. 2, 397–407.
- [AMMpr] P. Alberca-Bjerregaard, D. Martín-Barquero, C. Martín-González, *Inner derivations of exceptional Lie algebras in prime characteristic*, arXiv:1402.2212 [math.RA].
- [AS69] H.P. Allen and M.E. Sweedler, *A theory of linear descent based upon Hopf algebraic techniques*, J. Algebra **12** (1969), 242–294.
- [Cha41] H.J. Chang, *Über Wittsche Lie-Ringe* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941) 151–184.
- [Dix84] J. Dixmier, *Certaines algebres non associatives simples definies par la transvection des formes binaires* (French), J. Reine Angew. Math. **346** (1984) 110–128.
- [EK12] A. Elduque and M. Kochetov, *Gradings on the exceptional Lie algebras F_4 and G_2 revisited*, Rev. Mat. Iberoam. **28** (2012), no. 3, 773–813.
- [EK13] A. Elduque and M. Kochetov, *Gradings on simple Lie algebras*. Mathematical Surveys and Monographs **189**, American Mathematical Society, Providence, RI, 2013.
- [Far86] R. Farnsteiner, *The associative forms of the graded Cartan type Lie algebras*, Trans. Amer. Mat. Soc. **295** (1986) 417–427.
- [FN98] J. Feldvoss and D.K. Nakano, *Representation Theory of the Witt Algebra*, J. Algebra **203** (1998) 447–469.
- [HSpr] S. Herpel and D.I. Stewart, *Maximal subalgebras of Cartan type in the exceptional Lie algebras*, arXiv:1409.3861 [math.RA].
- [Hog82] G.M.D. Hogewei, *Almost-classical Lie algebras. II*, Nederl. Akad. Wetensch. Indag. Math. **44** (1982), no. 4, 453–460.
- [KMRT98] M.A. Knus, A. Merkurjev, M. Rost, and J.P. Tignol, *The Book of Involutions*, American Mathematical Society Colloquium Publications **44**. American Mathematical Society, Providence, R.I., 1998.
- [Nak92] D.K. Nakano, *Projective modules over Lie algebras of Cartan type*, Mem. Amer. Math. Soc. **98** (470) (1992).
- [Pre83] A.A. Premet, *Algebraic groups associated with Lie p -algebras of Cartan type* (Russian), Mat. Sb. (N.S.) **122**(164) (1983), no. 1, 82–96. English translation: Math. USSR-Sb. **50** (1985), no. 1, 85–97.
- [Sel67] G.B. Seligman, *Modular Lie algebras*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 40 Springer-Verlag, New York 1967.
- [SV00] T.A. Springer and F.D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, (2000).
- [Ste68] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968. Notes prepared by John Faulkner and Robert Wilson.
- [Str77] H. Strade, *Representations of the Witt Algebra*, J. Algebra **49** (1977) 595–605.
- [Wat71] W.C. Waterhouse, *Automorphism schemes and forms of Witt Lie algebras*, J. Algebra **17** (1971), 34–40.
- [Wat79] W.C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics **66**, Springer-Verlag, New York, 1979.

SCHOOL OF ENGINEERING AND COMPUTING SCIENCES, DURHAM UNIVERSITY, SOUTH ROAD,
DURHAM, DH1 3LE, UNITED KINGDOM

E-mail address: `alonso.castillo-ramirez@durham.ac.uk`

DEPARTAMENTO DE MATEMÁTICAS E INSTITUTO UNIVERSITARIO DE MATEMÁTICAS Y APLICACIONES,
UNIVERSIDAD DE ZARAGOZA, 50009 ZARAGOZA, SPAIN

E-mail address: `elduque@unizar.es`